EXHIBIT A

State of Illinois)
) ss
County of St. Clair)

UNSWORN DECLARATION UNDER PENALTY OF PERJURY IN SUPPORT OF COMPLAINT FOR FORFEITURE

I, Danny Allison, declare under penalty of perjury the following:

At all relevant times I have been a Detective Sergeant with the Caseyville Illinois Police Department and a Special Deputized Task Force Officer for the United States Secret Service ("USSS"). The contents of this Declaration are based on information provided to me during the course of my investigation from participants in the criminal activity, from other witnesses, and from other law enforcement officers.

1. On November 28, 2023, Officer Muennich with the Fairview Heights, Illinois Police Department was dispatched to the Fairview Heights Police Department in reference to a deceptive practice.

2. Upon Officer Muennich's arrival, he met with a male (D.B.) who advised Officer Muennich that on November 3, 2023, while checking his bank accounts through the GOOGLE Search Engine, he received a "pop up" notification advising him to call the Microsoft Fraud Department via phone number (762) 214-5388.

3. D.B. called the phone number and was provided with a "case number" of TA74282134. D.B. was transferred to a series of individuals attempting to assist him with the "fraud" that was currently on his bank account. An individual who provided the name of "Mr. Robin Ohsem" convinced D.B. to allow him to remotely connect to D.B.'s computer. "Mr. Robin Ohsem" then showed D.B. that his Schwab Investment Account currently had a balance of zero dollars. D.B. previously had a balance of $54,000 US Dollars in his Schwab Investment Account.

4. D.B. then was instructed by "Mr. Robin Ohsem" to withdraw $15,000 USD from his checking account at Regions Bank to refund his Schwab Investment account. D.B. was instructed by "Mr. Robin Ohsem" "not to talk to anyone, because someone might stop him from withdrawing the money." D.B. was instructed to tell bank employees that he was purchasing a boat with the funds, and that he was paying in cash.

5. Under the premise of this scam, D.B. withdrew a total of $58,900 US Dollars and deposited these funds into two different Bitcoin ATMs. D.B. made a total of five transactions in the month of November 2023. These transactions occurred on the following dates and times:

a. November 7, 2023, at 6:24 PM at a Bitcoin Depot BTC or Bitcoin ATM in the amount of $15,000 US Dollars;

b. November 10, 2023, at 1:52 PM at a Bitcoin Depot BTC ATM in the amount of $14,900 US Dollars;

c. November 13, 2023, at 2:34 PM at a Bitcoin Depot BTC ATM in the amount of $15,000 US Dollars;

d. November 20, 2023, at 2:04 PM at a Bitstop BTC ATM in the amount of $1,000 US Dollars; and

e. November 20, 2023, at 2:27 PM at a Bitstop BTC ATM in the amount of $13,000 US Dollars.

6. After one of the last transactions, D.B. was at Regions Bank located at 10950 Lincoln Trail in Fairview Heights, Illinois. A bank employee advised D.B. that he was likely the victim of a scam. The bank employee advised D.B. to contact the police.

7. On December 6, 2023, Detective Clay Mason with the Fairview Heights Police Department contacted declarant in reference to this case. Detective Mason provided the police report as well as the five Bitcoin ATM receipts of the transactions.

8. Using blockchain tracing software, I was able to trace the victims illicitly obtained Bitcoin. The suspect in this case attempted to use what is known as a "Peeling Chain" Technique. This technique involves sending portions of BTC or Bitcoin to several different

addresses to attempt to disguise the origin of the funds.

9. The suspect sent the victims illicitly obtained BTC to several different addresses. I was able to locate an address that was used as a hub to store the illicitly obtained BTC. As of December 7, 2023, this wallet address had a balance of 0.70626622 BTC, worth approximately $31,020 US Dollars.

10. The suspect made an outgoing transfer of approximately $720 US Dollars worth of BTC that had a portion of the victims illicitly obtained BTC to the address of:

3MuFxnT7nfmJMB8BpaZ19RFP1RSDqHHSX2

Transaction Hash: 5b55dc474343eab1b231d8947969f496326ba319920ea5a9a4c0d3db56796f4e

11. This transaction occurred on December 5, 2023 at 2:54 PM (UTC). This address has known attributions to the MEXC Global Crypto Currency Exchange. This address is linked to the suspect in this case.

12. I continued to trace the victims illicitly obtained BTC while the suspect was using the "peeling chain" method. Approximately $5,527 US Dollars' worth of BTC was sent to another address that is attributed to MEXC Global Cryptocurrency exchange. The suspect address that the victims BTC was transferred to was identified as:

3GqNKCd9ywpASfGUCGvhcW7XfniJGvHSDj

Transaction Hash: 877977d5171226dbbaf4f28154f21c6ec8a33a71c8d887dc2dd9daeff1aaeba5

This transaction occurred on November 29, 2023 at 8:39 PM (UTC).

13. I continued to trace the victims BTC and located another suspect address at MEXC Global Crypto Currency Exchange. This address had an incoming transfer of the victims illicitly obtained BTC in the amount of $20,186 US Dollars. This address was identified as:

32BamZ9jy5D1MPXTwSVcQ29QtqhCT2RHtA

Transaction Hash: 0eef6abb87ab6588e6b5bec7597e34a6511f27cf98fb49dc559af7ab63f2665c

This incoming transfer was on November 13, 2023 at 1:23 PM (UTC).

14. I continued to trace the victims BTC and located another address that was attributed to MEXC Global Cryptocurrency Exchange. This address had an incoming transfer of $26,319 US Dollars. This address was identified as:

3HDLYh1uYcoMre7MjvATNZDiLZ4uuKRwQp

Transaction Hash: 73308bc17e97ec3799975593a52cd9bcf9bf56fbe7a4699a2a5071e5eab17afe

This transaction occurred on November 16, 2023 at 6:11 PM (UTC).

15. I continued to trace the victims BTC and located an address at the Binance Cryptocurrency Exchange. This address had an incoming transfer of $20,418 US Dollars. This address was identified as:

19EVPeYQzL6BXXGb5rV8uY4WkZRdN63yKR

Transaction Hash: 7d785475dc5a20e6964c8d882c97996fbebd531ab905ee7167ed968d5a4e417c

This incoming transfer occurred on November 16, 2023 at 10:08 AM (UTC).

16. After learning that a large portion of the victim's funds were sent to an address at Binance Exchange, I contacted Binance and requested a temporary freeze and restraint request for the suspects address of **19EVPeYQzL6BXXGb5rV8uY4WkZRdN63yKR**. I also requested that any other addresses that are associated with the suspect be frozen.

17. I further requested information on the suspect known as KYC (Know Your Customer). This information includes name, address, phone number, email address, transaction logs, incoming and outgoing transactions, IP Logs, and anything else Binance could provide.

18. I also contacted an investigator with Binance and requested the current account balance of the suspect's account in reference to this case and was informed that the current account balance of the suspects account at Binance was approximately $80,000 in cryptocurrency.

19. Based upon my training and experience in cryptocurrency fraud investigations, I know that suspects often use more than one cryptocurrency wallet and account and move cryptocurrencies through multiple locations to disguise the source and ownership of the proceeds of wire fraud schemes.

20. After reviewing the facts of this case, all the assets within the suspect's wallets located at Binance are subject to forfeiture. A significant portion of the victim's illicitly obtained Bitcoin was transferred into Binance **User ID 36076314** on November 16, 2023, at 10:08:48 AM(UTC).

21. I know from experience in cryptocurrency investigations that those involved in cryptocurrency scams and fraud have an ultimate goal of getting the cryptocurrency to a cryptocurrency exchange such as Binance. The suspect that is attributed to BTC wallet address **19EVPeYQzL6BXXGb5rV8uY4WkZRdN63yKR** is very likely to be involved in the scheme to defraud the victim in this case.

22. The remaining funds within the suspect's wallet are likely a result of scams with other victims around the globe.

23. As of December 14, 2023, the suspect's BTC wallet address of **19EVPeYQzL6BXXGb5rV8uY4WkZRdN63yKR** had a total of $666,730 US Dollars worth of BTC deposited and withdrawn from this wallet address.

24. On December 13, 2023, I contacted an investigator with the cryptocurrency blockchain software company that developed the software that I used in this case. I requested that the investigator check the addresses linked to the suspect in this case through their internal database. The investigator advised me that they located an address that is known as a "Chip Mixer" that was used to deposit funds into the suspects BTC Address of **19EVPeYQzL6BXXGb5rV8uY4WkZRdN63yKR.**

25. A "Chip Mixer" is a cryptocurrency service that is used by those who wish to disguise the origin of their funds. For example, if you took 1 Bitcoin or BTC and deposited it in to a "Chip Mixer" address, the "Chip Mixer" address would provide you with 1 BTC back, but this Bitcoin would be in multiple small pieces of Bitcoin that the user could then transfer to multiple different addresses to disguise the origin of the 1 Bitcoin that was originally deposited. This is a method used by those who obtain Bitcoin illicitly. The origin of the funds within the suspect's wallets will continue to be investigated by law enforcement.

Identifying the Binance account of User ID 36076314

26. On December 11, 2023, I received account identifying information on the user with BTC Address **19EVPeYQzL6BXXGb5rV8uY4WkZRdN63yKR** from Binance. The user was identified as RISHI SIKRI from Ghaziabad, India. An identification card from the Republic of India with the name RISHI SIKRI contained a photo of a male of Indian Descent.

27. Binance documents indicated that the account associated with **User ID 36076314** had 16 different types of crypto currency in several different wallets. The total value of the assets in the user's wallets as of December 11, 2023, was $82,667.46 US Dollars.

28. Based on the user's account information, as well as identity documents and access logs, law enforcement does not believe the individual responsible for the fraud resides within the United States but is likely conducting the illegal activities from India.

29. Under 18 U.S.C. § 984, a court may order the forfeiture of funds in a bank account into which monies subject to forfeiture have been deposited, without the need to trace the funds currently in the account to the specific deposits that are subject to forfeiture, up to the amount of the funds subject to forfeiture that have been deposited into the account within the past one-year period.

30. Section 984 (a) provides in part:

> (1) In any forfeiture action in rem in which the subject property is cash [or] funds deposited in an account in a financial institution
>
> > (A) it shall not be necessary for the Government to identify the specific property involved in the offense that is the basis for the forfeiture; and
> >
> > (B) it shall not be a defense that the property involved in such an offense has been removed and replaced by identical property.
>
> (2) Except as provided in subsection (c), any identical property found in the same place or account as the property involved in the offense that is the basis for the forfeiture shall be subject to forfeiture under this section.

31. 18 U.S.C. § 984(b) provides: "No action pursuant to this section to forfeit property not traceable directly to the offense that is the basis for the forfeiture may be commenced more than 1 year from the date of the offense."

32. Thus, under Section 984, a court may order the civil forfeiture of monies found in a bank account into which deposits of criminal proceeds subject to forfeiture had been made, up to the amount of the forfeitable deposits that have been made into the account within the prior one-year period, without the need for tracing the funds to be forfeited to any of the specific forfeitable deposits.

33. On or about January 30, 2024, agents with the USSS seized the following cryptocurrency from Binance User ID 36076314:

a. 24566.937878 USDT;

b. 13411.9719 GTC;

c. 11678.4051 AGLD; and

d. 732196824.29 SHIB.

34. Based on the facts and circumstances set forth in this affidavit, I submit that there exists probable cause to believe that the cryptocurrency seized from Binance account **User ID 36076314**, and more fully described above:

a. Are funds traceable to, and are therefore proceeds of, a wire fraud offense or offenses, committed in violation of 18 U.S.C. § 1343;

b. Were involved in a money laundering violation of 18 U.S.C. § 1956 and 1957;

c. Are subject to civil forfeiture under 18 U.S.C. §§ 981(a)(1)(C);

d. Are subject to forfeiture in the United States under 18 U.S.C. sections 981(b) and 981(b)(3).

Pursuant to 28 U.S.C. § 1746(2), I declare under penalty of perjury that the foregoing is true and correct.

Executed on this 15th day of February, 2024.

Dt. Sgt. Danny Allison #536

Danny Allison
Task Force Officer
United States Secret Service